B1 fraudulent data can be eliminated as the received data format conversion means can convert data with an external format to data with reliable internal format.

IN THE SPECIFICATION:

Please replace the entire text of the specification with attached substitute specification. A marked-up version of the specification showing the matter being added and the matter being deleted is also attached.

REMARKS

Applicants request entry of this second Preliminary Amendment prior to examination of the present application. The Abstract has been amended to remove reference numerals from the Abstract and use proper idiomatic English. To provide a specification that is in proper form and that uses proper idiomatic English, a substitute specification is attached to and submitted with this preliminary amendment. A marked-up version of the specification showing the matter being added and the matter being deleted from the specification is attached. No new matter has been added.

In view of the foregoing, it is respectfully submitted that the application is in condition for allowance. If for any reason the Examiner finds the application other than in condition for allowance, the Examiner is requested to call the undersigned attorney at the Los Angeles, California telephone number (213) 337-6700 to discuss the steps necessary for placing the application in condition for allowance.

If there are any fees due in connection with the filing of this response, please charge the fees to our Deposit Account No. 50-1314.

Respectfully submitted,
HOGAN & HARTSON L.L.P.

Date: January 10, 2002

By: _____
Ying Chen
Registration No. P-50,193
Attorney for Applicant(s)

500 South Grand Avenue, Suite 1900
Los Angeles, California 90071
Phone: 213-337-6700
Fax: 213-337-6701

09/921729

[[Name of Document] Specification]

NETWORK SECURITY SYSTEM

[[Title of the Invention] Network security system

[Industrial Applications]]

BACKGROUND OF THE INVENTION

The present invention is related to [a] network security [system to]systems, and more particularly to network security systems that can protect an internal system [which sends and receives data through a network from the network.] that can send and receive data over a network.

[[Background technology]

In a system such as one] In systems that can be used for the sale of goods [in use in such]via networks such as the Internet, sales [administration such as one which arranges goods and delivers it are conducted by obtaining] and delivery of goods can be conducted to obtain order information through the network [and writing the]. The sales information can then be written to a database. In such a system, [in case the]the data representing customer order information can be damaged during fraudulent acquisition of the data representing customer order information by hackers. In turn, customers orders can be suspended and/or lost. Moreover, when customer order information is [damaged through the acquisition of fraudulent data from the network, order obtaining activity is suspended, and extreme damage may occur. Also in the case where customer information is stolen through the network by a fraudulent means,] fraudulently stolen through the network, significant credit problems [occur. Therefore, a security system, known as a firewall, is] can occur for consumers. Conventionally, security systems known as firewalls are placed between the network and the internal system to [prevent the invasion of hackers and the like.] reduce and/or prevent the likelihood of invasion by hackers.

[In the prior art of technology described above, the following problems must be overcome.

A firewall requires] Conventional firewall technology can require identification information [and], security [code and the like] codes and authentication to ensure [the right to] access for those about to access the Internal system through the [network.(Patent] network. Such firewall technology is described, for example, in patent publications 11-298639, and 10-214304). However, it [is not easy]-can be difficult to protect against hackers who obtain identification information and security [code] codes by

fraudulent means [and camouflage. Moreover, in the ways to obtain the order information from general run of users and take them into the database such as the system of order and sales of goods, a] and/or camouflage. To encourage general customers to place orders over the Internet, an ordering system is necessary [to assure the elimination of fraudulent data about to become mixed with the order information. Also, a system is necessary to assuredly eliminate actions for fraudulently reading the contents of the database.]that can reduce and/or prevent fraudulent data from becoming mixed with the data representing customer order information. Accordingly, a system is needed that can reduce and/or eliminate fraudulent reading of the contents of a database used in a system for sales of goods over a network.

[[Description of the invention]]

SUMMARY OF PREFERRED EMBODIMENTS

[The present invention adopts the following constructions to resolve the problems stated above.

<Construction 1>

A] An aspect of the present invention relates to a network security system [comprising] is provided that includes a server connected to a [net work] network, a received data storage means to store data with an external format which a server received through the [new work] network, a received data format conversion means to convert data with an external format stored in the received data storage means to data with the internal format and to store them in a received-process data storage means, and a host computer to execute a predetermined process utilizing data with internal format stored in the received-process data storage means.

A server is connected to the network. Data with an external format is received from other terminal units through the network. The data format of data with the external format is optional. The data format of data with the internal format is optional as well.

The received data format conversion means reads out data with the external format from the received data storage means and converts them to data with the internal format in a fixed procedure, and afterwards, writes them in the received process data storage means. Data with the internal format stored in the received process data storage means are utilized by the host computer. The received data format conversion means extracts and fabricates only necessary data from the data with an external format, and converts them to internal data with the predetermined and reliable format.

Data with an external format received through the network is written in the received data storage means, but the host computer does not directly access to the received data storage means. [This is why] As a result, obtaining [in] fraudulent data can be prevented. [Namely, when] When the received data format conversion means converts data with an external format to data with an internal format, [it] the received data format conversion means can convert the data with the external format to internal data with a reliable format, thereby eliminating the fraudulent data. The host computer can access the received process data storage means with selective timing and use the data with the internal format.

[<Construction 2>

A network security system according to construction 1, wherein] According to another aspect of the present invention, the received data storage means [allows] can allow data with an external format which the server received to be written, and [prevents] can reduce the likelihood of and/or prevent data from being read out by the server[, a]. A received process data storage means [allows] can allow data with an internal format to be read out by the host computer and [prevents] can reduce the likelihood of and/or prevent data from being written by the host computer. [

]The [reason the] received data storage means [prevents] can reduce the likelihood of and/or prevent data from being read out by the server is [to prevent] by reducing the likelihood of and/or preventing the data in the received data storage means from being read out from the network side. [The reason] Preventing writing data into the received process data means by the host computer [is prevented is to] can reduce the likelihood of and/or prevent data from being carelessly output from the host computer side to the network side. This [prevents the flow of data]can reduce the likelihood of and/or prevent data from flowing from the host computer to the network[, and data]. Data on the host computer side is not read out to the network side. [All data are prevented from] The likelihood of data being written or read out can be reduced and/or prevented. This includes all formats of data, whether internal or external.

[<Construction 3>

A network security system according to construction 1 or 2, wherein] According to another aspect of the present invention, the received data storage means [allows] can allow data with an external format to be read out by the received data format conversion means and [prevents] can reduce the likelihood of and/or prevent data from being written by the received data format conversion means, and the received process data storage means allows data with an internal format to be written by the received data format

conversion means and [prevents] can prevent data from being read out by the received data format conversion means. [

]The received data format conversion means is allowed only to read out data with an external format from the received data storage means, and only to write data with the internal format to the received process data storage means.

As a result, [This makes] data flow by the received data format conversion means is a one way flow from the network side to the host computer side. Then, the data flow from the host computer side to the network side [is] can be prevented, and data on the host computer side [is protected.] can be protected.

[<Construction 4>

A network security system according to any one of constructions 1 to 3, wherein] According to another aspect of the present invention, the data with the internal format [are] can additionally be stored at predetermined times into the database of the host computer from the received-processing data storage means.

When [In case] the received process data storage means is arranged [with] apart from the host computer, data corresponding to the database of the host computer side [are] can be transferred from the received process data storage means. Data can be transferred with predetermined timing, independent from action of the received data format conversion means. The timing of updating the database on the host computer side is optional.

[<Construction 5>

A network security system according to construction 4, wherein] According to another aspect of the present invention, the conversion process from data with an external format to data with the internal format by the received data format conversion means and the additional storage process of the data with an internal format to the database of the host computer are respectively executed in a composite manner, with an independent timing. [

]Writing the received data in the received data storage means by the server is usually done with each piece of data. But the received data format conversion means executes the conversion process compositely. What is meant by composite execution is that processing occurs not of piece of data, but as a composite numerical number of data, such as occurs in a batch process. What is meant by execution with independent timing is that the activation control of each process is independent. There is no problem, of course, if controlling the activation timing is intended, for instance, in a

manner in which the additional storage process initiates to the database of the host computer side automatically when the conversion process of the received data format conversion means is terminated.

[<Construction 6>

A network security system according to any one of constructions 1 to 3, wherein] According to another aspect of the present invention, the received data format conversion means [converts] can convert data with an external format to data with a database format. [

]Only the essential conversion process is executed to obtain data received from the network in the database processing with the host computer. Therefore, obtaining fraudulent data in the host computer side can be prevented.

[<Construction 7>

A network security system according to any one of constructions 1 to 3, wherein the server sends] According to another aspect of the present invention, the server can send data with a mail format to the received data storage means and [writes] can write data with an external format. [

]The way that the server sends data with mail format to the received data storage means secures one-way flow of data to the received data storage means from the server more than the way that the server writes data with an external format by accessing the storage region of a storage device.

[<Construction 8>

A network security system according to any one of constructions 1 to 3, wherein] According to another aspect of the present invention, the network is the Internet. The Internet [requires] can require much higher security [among intranets. That is why this system is adopted.] than intranets.

[<Construction 9>

A] An aspect of the present invention provides a network security system [comprising] that can include a host computer to execute a predetermined process by using data with an internal format, a transmit process data format conversion means to storage data sent to the network, a transmit data format conversion means to convert data with an internal format stored in the transmit process data storage means and to store them in a transmit data storage means, and a server to send data with an external format stored in the transmit data storage means to the network.

A server is connected to the network. Data with an external format is sent to other terminal devices through the network. The ways of data with an external format and its data format type, data with the internal format and its data format type, and conversion of the data format type are the same as in the case of received data. The received data format conversion means reads data with the internal format from the transmit process data storage means and converts them to data with an external format in a fixed procedure, and then, writes them to the transmit data storage means.

The host computer writes data with the internal format to be sent to the transmit process data storage means with selective timing. Data with an external format sent from the server through the network is written by the transmit data format conversion means in the transmit data storage means. The server does not directly access to the transmit process data storage means. That is why accidentally sending out data to be protected on the host computer side can be prevented.

[<Construction 10>

A network security system according to construction 9, wherein] <u>According to another aspect of the present invention,</u> the transmit process data storage means [allows] <u>can allow</u> data with an internal format to be written by the host computer and [prevents] <u>can prevent</u> data from being read out by the host computer, and the transmit data storage means [allows] <u>can allow</u> data with an external format which the server sends to be read out and [prevents] <u>can prevent</u> data from being written by the server. [

]The [reason the] transmit data storage means [prevents] <u>can prevent</u> data from being read out by the host computer [is to]<u>in order to reduce the likelihood of and/or</u> prevent fraudulent data from invading from the network side. The reason writing data into the transmit data storage means by the host computer is [prevented is to prevent] <u>that the likelihood of</u> fraudulent data from invading from the network side <u>can be reduced and/or prevented</u>. This secures only the data flow from the host computer to the network, and the internal system including the host computer is protected. All data [are] <u>can be</u> prevented from being written or to be read out. All formats of data are included regardless of the type.

[<Construction 11>

A network security system according to construction 9 or 10, wherein] <u>According to another aspect of the present invention,</u> the transmit process data storage means [allows] <u>can allow</u> data with an internal format to be read out by the transmit data format conversion means and [prevents] <u>can prevent</u> data from being written by the transmit data format conversion means, and the transmit data storage means [allows] <u>can allow</u> data with an

external format to be written and [prevents] can prevent data from being [read out] readout by the transmit data format conversion means. [

]The transmit data format conversion means is allowed only to read out data with internal format from the transmit data storage means, and only to write data with an external format to the transmit process data storage means. [This manner makes the] As a result, data flow by the transmit data format conversion means [to be] is a one way flow from the host computer side to the network side. Then, data flow from the network side to the host computer side [is] can be prevented, and data in the host computer side [is protected.] can be protected.

[<Construction 12>

A network security system according to any one of constructions 9 to 11, wherein] According to another aspect of the present invention, the conversion process from data with the internal format to data with an external format by the transmit data format conversion means [is] can be executed with independent timing from the storage process of data with the internal format to the transmit process data storage means by the host computer. [

]The transmit data format conversion means can execute the conversion process with selective timing since the transmit process data storage means is arranged. Also, the host computer can write data with an internal format for sending with selective timing into the transmit process data storage means. The format of the internal data for sending is optional, and is not limited to database formats.

[<Construction 13>

A network security system according to any one of constructions 9 to 11, wherein the server receives] According to another aspect of the present invention, the server can receive data with mail format from the transmit data storage means and [sends] can send them to the network. [

]The way that the server sends data with mail format to the transmit data storage means [secures] can secure one way flow of data to the transmit data storage means from the server more than the way that the server writes data with an external format with accessing the storage region of a storage device.

[<Construction 14>

The network can be, for example, [A network security system according to any one of constructions 9 to 11, wherein the network is] the Internet. [

]The Internet [requires] can require much higher security compared with an ordinary intranet. [That is the reason for adopting this system.

<Construction 15>

A] An aspect of the present invention can also provide a network security system [comprising] that includes a received data storage means to storage data with an external format which a server received through the network, a received data format conversion means to convert data with an external format stored in the received data storage means to data with an internal format and to store them in the received process data storage means, a host computer to execute a predetermined process by using data with the internal format stored in the received process data storage means, a transmit process data storage means to store data with the internal format sent to the network, a transmit data format conversion means to convert data with the internal format stored to the transmit process data storage means to data with an external format, and a server to send data with an external format stored in the transmit data storage means to the network. Other aspects of the present invention can be arranged in the system stated in this aspect of the invention.

[The function of data received in construction 1 and the function of data sending in construction 9 are both arranged in the system stated here.]

[<Construction 16>

A network security system according to construction 15, wherein] According to another aspect of the present invention, the conversion process of from data with an external format to data with the internal format by the received data format conversion means, the additional storage process of the data with the internal format to the database of the host computer side, the conversion process from data with the internal format to data with an external format by the transmit data format conversion means, and the storage process of data with the internal format to the transmit process data storage means by the host computer are each [are] executed with independent timing. [

]As a barrier to one way flow is arranged in this manner, and data transfer is executed in order with each independent timing, protection of the host computer side from the network is reinforced. This has the effect that there is no way to send a fixed command from the network side using the data receiving function in construction 1 and to read out some data from the host computer side using the data sending function.

[<Construction 17>

A] An aspect of the present invention can provide a network security system comprising a server connected to the network and a mail transfer section connected to a host computer side, wherein a mail client and a mail server are arranged in the server, a mail receiving section to receive mail through communication line from the mail client and a mail sending section to send mail through the communication line to the mail server are arranged in the mail transfer section, and the host computer receives a data transfer from the server through the mail receiving section of the mail transfer section and transfer data to the server through the mail sending section of the mail transfer section. [

]Data transfer between the server and mail transfer section [are] can be implemented only with a fixed mail format. The host computer [gives] can give and [takes] take data with the server only through the mail transfer section. [That is why] As a result, there is no way for fraudulent commands or fraudulent programs to be transferred between the server and the mail transfer section.

[<Construction 18>

A network security system according to construction 17, wherein] According to another aspect of the present invention, the communication line [is] can be a communication line dedicated to mail. [

]Connection between the server and the mail transfer section with a communication line which is dedicated to mail and does not have a path for other data invading and can thereby help maintain security with more certainty.

[<Construction 19>

A] An aspect of the present invention can provide a network security system comprising a mail server arranged on the network side and a mail transfer section arranged on the host computer side, wherein a mail receiving section to receive mail from the mail server through a mail dedicated line and a mail sending section to send mail to the mail server through a mail dedicated line are arranged, and the host computer receives data transfer from the mail server through the mail receiving section of the mail transfer section and transfers data to the mail server through the mail sending section of the mail transfer section.

The mail server is arranged on the network side, and sends and receives mail through a dedicated line between the mail server and the mail transfer section of the host computer side. A dedicated line is optional if a line is a

communication line, which would be only used for communication between the mail server and the host computer side. The host computer is protected from the network side, because the dedicated line is used for data transfer between the network and the host computer only by a fixed means.

[[Brief explanation of drawings]]

BRIEF DESCRIPTION OF THE DRAWINGS

[Fig.1] Fig. 1 is a block diagram showing [the] an example of the system related to the present invention.
[Fig.2 is an explanation drawing to explain] Fig. 2 shows the actions of the process that data the server received are converted and stored in the received process data means.
[Fig3] Fig. 3 is a flow chart of the actions with the server and the received process data storage.
[Fig.4] Fig. 4 is a block diagram indicating the example using the present invention to the system for the sending process.
[Fig.5] Fig. 5 is a block diagram of the system further reinforcing the security function.
[Fig.6] Fig. 6 is another system of block diagram reinforcing the security function by use of mail sending.

[[Embodiment]]

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

[As follows, embodiment related to the present invention is explained in use of examples.] The present invention now will be described more fully hereinafter with reference to the accompanying drawings, in which preferred embodiments of the invention are shown. This invention may, however, be embodied in many different forms and should not be construed as limited to the embodiments set forth herein; rather, these embodiments are provided so that this disclosure will be thorough and complete, and will fully convey the scope of the invention to those skilled in the art. Like numbers refer to like elements throughout.

[<Receiving process>]

Receiving Process

[Fig.1] Fig. 1 is a block diagram showing an example of the system of the present invention. [

]As shown in the [figure] Fig. 1, the various terminal devices 2 which users utilize are connected to [the terminal 2] a network 1. A system for providing

information for purchasing goods, for instance, [is] can be connected to the network 1. This system [constitutes the] can be, for example, a network security system 20 to reinforce the protection function by the present invention. The network security system 20 [comprises] can comprise a server 3, received data storage means 6, received data format conversion [means7] means 7, received process data storage means 8 and a host computer 10.

The server 3 is connected to the network 1. Inside of the server 3, a storage device, not shown, adapted to store [the] information to provide users [is], can be installed. This network [is] preferably [applied to] comprises the Internet, but can [be applied to] include all other networks other than internet, such as a telephone network specifying users, and intranet.

When an order is [place] placed by a user, the server 3 typically receives the order information through the network 1. The host computer 10 is placed to process the order information and to arrange and [administrate] administer goods. The received data storage means 6, the received data format conversion means 7, and the received process data storage means 8 transfer the order information received by the server to the host computer 10. The host computer 10 [stores] can store the order information in the database storage section 9 from the received process data storage means 8 and [administrates] can administer the orders.

The received data storage means 6 [comprises] can include a storage device for storing the data with an external format 4 which the server 3 receives through the network. The data with an external format 4 [is what is] can be received from other terminal devices through the network, whose format is an optional format such as an e-mail format and a data file format. Also data [with] having a text type of format, or data [with] having a binary type of format [is] can also be applicable. The received data format conversion means 7 [has the function of reading] can read data with an external format 4 from the received data storage means 6, [to convert it] convert the data with the external format 4 to the data with the internal format 5 in a fixed procedure, and [then to write it] can then write the data with the internal format 5 in the received process data storage means 8. The received data format conversion means 7 [should be] is preferably implemented by computer programming, but can also be implemented by hardware. Conversion of data format can be arranged optionally including extraction, sorting, partial delete, data addition, and the like. The received data format conversion means 7 [has the effect of filtering] can filter fraudulent data contained in the received data as the received data format conversion means 7 does not simply transfer data [simply].

The format of the data with the internal format 5 is optional as well, but the data has a fixed format pre-regulated on the host computer side. In this

example, data with a CSV format is applied, because [with] the CSV format can make it [is] easy to update the database stored in the database storage section 9. Data with the CSV format are data with a text type format. The received data format conversion means 7 [analyses] can analyze data received with an external format the server 3 [received, extracts], extract the necessary data items and [generates] generate data with the internal format. The received process data storage means 8 is typically a storage device adapted to store fixed amounts of data with the internal format 5 [and hold them], and hold fixed amounts of data with the internal format 5 until the data with the internal format 5 is written in the database storage section 9.

Fig 2 [is an explanatory drawing to explain the action in which data the server received is converted into the] shows conversion of data received by the server into data being stored in the received process data storage means. Fig. 3 is a flow chart [of the] illustrating actions [with] of the server and the received process data storage means. Conversion will now be[, and the like.

The actions are] explained [hereafter,] with reference to the drawings. First, the server [writes] can write data D1 received from the network 1 in the order [in] the received data is received by storage means 6 [(Fig.3](Fig. 3, step S1, step S2). Data D2 accumulated in the received data storage means 6 [is] can be read out by the received data format conversion means 7 at fixed intervals, and [undergoes the conversion process] can be converted to the data with the internal format 5 from the data with an external format 4 [(Fig.3](Fig. 3, step S3, step S4).

For instance, in case of administration of ordering data, this conversion process is set up to be executed once [during night each] a day, twice a day, or every other hour. Therefore, the received data format conversion means 7 [should] can preferably monitor the system timer and commence the action when the time for starting conversion [starting] is up.

In the case of administration of ordering, data with mail format containing data on user codes, ordered goods codes, quantity to be ordered, and the like [are], for example can be stored in the received data storage means. If data indicating the location of the user code, for instance, is contained in the data with an external format, the data can be detected and cut off[. And], and only the portion of the user code can be extracted. At this time, [as the] parts other [parts] than the user code and necessary data [are] can be cut off and thrown away automatically. As a result, obtaining fraudulent data can be prevented. [When obtaining] Obtaining camouflaged data, [if] by inspecting a format with the data [is inspected, obtaining camouflaged data], can be prevented. The received data format conversion means 7 [extracts] can extract the necessary data items in this manner, and [generates] can

generate a text format of data separated, for instance, by commas. This data is written in the received process data storage means 8.

When the conversion process of all data D2 stored in the received data storage means is finished, the program goes [to step S6] from step S5 in Fig. 3 to step S6 and the updating process of the database is executed. Data D3 stored in the received process data storage means 8 are written in the database as [they are. In case] is. When the data D3 are data with CSV format [stated above, they], the data D3 can be taken into the database as [they are] is and can be used for organizing received orders.

In the example above, after the [conversion process of] data with an external format 4 is converted to data with the internal format 4 by the received data format conversion means 7, the storage process of this data with the internal format for addition to the database on the host computer side [are] can be executed. However, these processes should be executed independently for the convenience of system operation. The conversion process by the received data format conversion means 7 is preferably executed when data with an external format is accumulated in some amount or when access to the server is not so busy.

The server usually writes the received data in the received data storage means with one piece of data. [What is meant by] As used herein, composite execution [is] refers to [be processed] processing not for each piece of data but a composite of numerical number of data, as with a batch process. [What is meant by] As used herein, execution with independent timing [is the] refers to independent activation control of each process.[. There is no problem, of course, if controlling the] Nevertheless, activation timing [is] intended to control, for instance, in a manner in which an additional storage process initiates to the database of the host computer side automatically when the conversion process of the received data format conversion means is terminated, may also be acceptable.

The received data format conversion means 7 is not just an interface between the server and the host computer. [It has the function of a filter for] The received data format conversion means 7 can also filter the one-way flow to extract and fabricate only the necessary data from data with an external format which might contain fraudulent data, and [to] can convert [them] the necessary data to data with pre-established, safe, and internal format. Data with an external format the sever 3 received through the network 1 (shown in Fig. 1 [is]) can be written into the received data storage means 6. The host computer 10 does not [make direct] directly access [to] this received data storage means 6. [That is why] As a result, the host computer 10 can be prevented from obtaining fraudulent data from the network 1.

In Fig. 1, the received data storage means 6 can be a storage device set up to be independent from the server 3, or can be part of the storage device arranged inside of the server or the host computer 10. The received process data format conversion means 8 as well can be a storage device set up independently from the server or the host computer 10, or can be part of the storage device arranged in the inside of the host computer. The received data format conversion means 7 can be a computer program working on the server 3 or a computer program [working] adapted to be executed on the host computer 10.

Furthermore, the received data storage means 6 could allow data with an external format received by the server 3 [received] to be written, but should prevent all data from being read out by the server 3. This can be implemented, for instance, by [a well known function] functions of the operation system. [Or] Alternatively, as will be explained later, the server 3 [should] can transfer data with a mail format to the received data storage means 6. This can prevent data in the received data storage means 7 from being read out from the network side. The received process data storage means 8 could allow data with the internal format to [being] be read out by the host computer 10, but [should] can prevent [all] data from being written by the host computer 10. [

]Working of the received data format conversion means 7 can be limited as well.

[Namely the] The received data storage means 6 [allows] can allow data with an external format to be read out by the received data format conversion means 7, [while preventing] can also prevent all data from being written by the received data format conversion means 7. The received process data storage 8 [allows] can allow data with the internal format to be written by the received data format conversion means 7, [while preventing] and can also prevent all data from being read out by the received data format conversion means 7. As stated above, it [is] may be feasible to effectively protect the internal system from hackers by arranging several barriers with one way flow.

[<]Sending [process>]Process

[Fig.4] Fig. 4 is a block diagram showing the [example] one preferred implementation of a system for sending [process]. The system shown in [Fig.1 takes] Fig. 1 can safely take data received through the network into the database processed by the host computer [safely. This can apply to the case of], for example, when sending data from a host computer to a network. [Fig.4] Fig. 4 is one such example. The blocks the system in Fig. 1

[comprises] appearing in Fig. 4 are denoted with a dashed line for purposes of distinction.

In the system in [Fig.4] Fig. 4, the host computer 10 has the received data storage means 12, the received data format conversion means 13 and the transmit process data storage means 14. The [rest is the same as] remained of the system is similar to the system shown in Fig. 1. The host computer 10 [executes] is adapted to execute ordering administration and the like in the use of the database storage section 9. The received process data storage means 14 [is] can be a storage device to store data with the internal format which the host computer generates and [sent to] sends over the network. The transmit data format conversion means 13 [has a function] is adapted to convert data with the internal format stored in the transmit process data storage means 14 to data with an external format and to create the data stored in the transmit data storage means 12. This, as well as the example in Fig. 1, [comprises the] can comprise a computer program and the like. The server 3 [has a function] is adapted to send data with an external format stored in the transmit data storage means to the network. The content and format of data with an external format and internal format is generally the same as the example in Fig. 1.

In this system, if the host computer 10 has data to be sent through the network, the host computer [converts] can covert this to the data with the internal format with selective timing and [makes it stored] can store the data in the received process data storage means 14. The transmit data format conversion means 13 [is] can be, for instance, activated in each case by the host computer, and [reads] can read out data with the internal format from the transmit process data storage means 14 and [converts it] convert data with the internal format to data with an external format. [And then, it writes it] The transmit data format conversion means 13 can then write data with an external format to the transmit data storage means 12. This action is different from the case of data received in Fig. 1. As the transmit data format conversion means 13 can acquire information on emergency of sending data from the host computer, the timing of sending data should be classified.

After data are written in the transmit data storage means 12, the server should conduct a sending process to the network with emergency of data sending considered, as well. In this example also, the transmit process data storage means 14 allows data with the internal format to be written by the host computer, and should prevent data from being read out by the host computer. The transmit data storage means 12 can preferably [allows] allow data with an external format sent by the server to be read out, and [prevents] can prevent data from being written by the server 3.

Furthermore, the transmit process data storage means 14 can preferably [allows] allow data with the internal format to be read out by the transmit data format conversion means 13, [while should] and can prevent data from being written by the transmit data format conversion means 13. The transmit data storage means 12 can preferably [allows] allow data with an external format the server sends to be written by the transmit data format conversion means 13, [while preventing] and can prevent data from being read out by the received data format conversion means 13. As stated above, it is feasible to prevent hackers from stealing data by arranging several barriers with one way flow to the network.

The conversion process of data with the internal format to data with an external format by the received data format conversion means 13 can be executed with independent timing from the storage process of data with the internal format to the transmit process data storage means 14 by the host computer 10. The system combining the system to receive data indicated in [Fig.1] Fig. 1 and the system to send data indicated in Fig. 4 can present extremely high security as far as received and [transmit] transmitted data is concerned. It is preferable that the conversion process by the received data format conversion means 7 shown in [Fig.4] Fig. 4, the additional storage process of data with the internal format to the database of the host computer 10 side, the storage process of data to the received process data storage means 14 by the host computer 10 and the conversion process by the received data format conversion means 13 are each [are] preferably executed with independent timing.

[Fig.5] Fig. 5 is a block diagram [to more] of a network security system that greatly [reinforce] reinforces the security [function] of the system.

Typically [Usually], a specified region in the storage device of a computer can be controlled with only reading out, and the rest of region in the storage device can be controlled [with] by preventing both reading out and writing [being prevented]. However, it [is not easy] can be difficult to prevent hackers from invading the system completely by a fraudulent means [as] when this kind of control is accomplished by software. For instance, if each function block shown in the system of [Fig.1] Fig. 1 is brought into practice using a single computer, it would be the same as if the received data storage means 6, the received process data storage means 8, the transmit data storage means 12 and the transmit process data storage means 14 were all located on one memory. The server 3 and the host computer 10 could be connected directly by LAN (Local Area Network) and share a storage device. In such a case, it would [not] be [easy] difficult to prevent fraudulent access completely [to] by the received process data storage means 8 and by the transmit process data storage means 14, which should be protected on the host computer side. [

]Therefore, in this example, a mail system which can transfer only with a fixed format, [is] can be used to connect between the server and the host computer.

The server in [the Figure] Fig. 5 has [the] a mail client 31, [the] a storage device 33 and [the] a mail server 32. Also, [the] a mail transfer section 40 has [the] a mail receiving section 41 and [the] a mail sending section 42. Further [the] a data conversion section 50 has [the] a received data storage means 6, [the] a received data format conversion means 7, [the] a received process data storage means 8, and [the] a transmit data storage means 12. In the example, the function of the mail transfer section 40 stated above controls a way to transfer data in the sever 3 and the data transfer of the host computer side to reinforce the security of the host computer side. If the data transfer section 50 is arranged with the mail transfer section 40, it could [secure] provide higher system security [of the system].

The mail receiving section 41 of the mail transfer section 40 [is] can be a device [to have] having a mail receiving function, and the mail sending section 42 [is] can be a device [to have] having a mail sending function. These mail transfer section 40 and the server 3 are preferably connected only with cables for mail receiving and sending 43, 44. Data transfer between the server 3 and the mail transfer section 40 are typically not executed without a fixed mail format under this configuration. For instance, if the data format transferred with this mail is limited [with] to a text format of data, [it would not occur that] fraudulent commands and [program are] programs would not be transferred between the server 3 and the mail transfer section 40.

[The system described above works as follows.

]In the storage device 33 of the server 3[, for instance,] web page data, for example, such as a home page to sell goods through the network 1 such as the [internet are] Internet can be stored. The mail client 31 sends data to place an order for goods to the mail receiving section 41 of the mail transfer section 40 with a mail format[, when]. When the mail client receives [it] orders for goods from users with the terminal device 2 through the network[. The], the mail receiving section 41 has the received mail to be stored in the received data storage means 6.

[As has been explained, in the following process, the data is] The data can then be taken in the database 9 after the conversion of data format. The data conversion section 50 can comprise, for example, a means to convert the data format to the database format and write database 9 directly. [

]On the other hand, [in case] when an order is being placed, the host computer [generates] can generate a comment [telling us 'Receiving] reading "Receiving an order" [and] with delivery information including a shipping

date. This comment and information [are] can be stored in the transmit data storage means 12. The mail sending section 42 [sends] can send this comment [an] and information to the mail server 32 after this comment and information are converted to data with mail format. The mail server 32 [sends] can then send the data to the network.

In other words, the mail client 31 [sends] can send data with the mail format to the mail receiving section 41, but does not have a mail receiving function [to receive mails]. The mail server 32 receives mails from the mail sending section 42 but does not have a mail sending function [to send mails]. A dedicated communication line for transferring should be used to make connection between the server 3 and the mail transfer section 40. [By this way] As such, the server 3 and the mail transfer section 40 can be constituted separately [in hardware's] from a hardware point of view. To enhance the security even more, the [The] communication line is preferably one which does not have a invading route of other data [to enhance the security more]. As only data with mail format, not data with the other format is transferred, [there is no way that] and fraudulent commands or data [are] can not be taken [in] to the host computer and the like. Therefore, to provide enhanced reliability, this communication line is preferably a one-way data transfer path [with reliability. This will provide the function of high protection to the system requiring high]. This can provide the improved system security.

Fig. 6 is a block diagram [with another system to reinforce the security by use of mail transfer. In the example of this figure,] of another system using mail transfer to improve security. The web server 51 of the system 20 is connected to the network 1 and [makes communication] can communicate with the network 1. This web server 51 is connected to the mail server 52. The mail server 52 is connected to the mail receiving section 41 of the mail transfer section 40 through the mail dedicated line 53. [And the] The mail server 52 is connected to the mail sending section 42 of the mail transfer section 40 through the mail dedicated line 54. The portion below the mail transfer section 40 to the host computer is the same as [Fig.5.] Fig. 5. This system [is ensured to have enough] can help to ensure high security whether the mail transfer section 40 is connected to the host computer directly or the mail transfer section 40 is a part of the host computer 10.

The mail-dedicated lines 53, 54 above, are used only for transfer of mail between the mail server 52 and the mail transfer section 40. These lines cannot transfer data with any format but a specified one, as these lines are used only for mail transfer. Therefore, illegal invasion from the network side to the host computer side can be assuredly prevented. [It will not happen that data are] Data are not carelessly sent out from the host computer to the network [carelessly]. The dedicated lines 53, 54, can be made up of a separate [cable for upward and downward as in the figure] upstream and

downstream cables as shown in Fig. 6 or can be made of one cable capable of transferring mail in both directions. [Also in this example, for convenience of the explanation above, arrows are indicated for data]Arrows indicate that data is to be transferred only in one direction from the network 1 to the web server 51. [But] Nevertheless, communication between the network 1 and the web server 51 can be made in both directions.

In the system stated above, when data to place orders for goods from the terminal 2 is sent to the network 1, the web server 51 receives [it] the order. The web server 51 [sends] can send the received data to the mail server 52[. The], and the mail server 52 [sends] can send the data to the mail receiving section 41 through the dedicated line 53 with mail format. On the other hand, mails sent from the host computer 10 [are] can be transferred to the mail server 52 through the dedicated line 54 from the mail sending section 42. The mail server 52 [sends] can send the mail to the terminal device 2 through the network 1 in use of the own function of mail receiving. The [rest of the parts are the same as has been already explained, and a superfluous explanation is omitted. In this manner, the mail] remaining parts are similar to those described above, and for sake of brevity will not be repeated. Mail transfer by use of the dedicated lines 53, 54 can provide protection and reinforcement of the internal system from the network.

Various aspects of the present invention have been illustrated in detail in the figures. It will be understood that individual blocks of the figures, and combinations of blocks in the figures, can be implemented by computer program instructions. These computer program instructions may be provided to a processor or other programmable data processing apparatus to produce a machine, such that the instructions which execute on the processor or other programmable data processing apparatus create means for implementing the functions specified in the block or blocks. These computer program instructions may also be stored in a computer-readable memory that can direct a processor or other programmable data processing apparatus to function in a particular manner, such that the instructions stored in the computer-readable memory produce an article of manufacture including instruction means which implement the functions specified in the block or blocks.

Accordingly, blocks of the figures support combinations of means for performing the specified functions, combinations of steps for performing the specified functions and program instruction means for performing the specified functions. It will also be understood that individual blocks of the figures, and combinations of blocks in the flowchart illustrations, can be implemented by special purpose hardware-based computer systems which perform the specified functions or steps, or by combinations of special purpose hardware and computer instructions.

In the drawings and specification, there have been disclosed typical preferred embodiments of the invention and, although specific terms are employed, they are used in a generic and descriptive sense only and not for purposes of limitation, the scope of the invention being set forth in the following claims. [Each function block indicated in each figure can comprise each separate program module, or can be composed of an integrated program module. The whole or part of these function blocks can comprise a hard ware by a logical circuit. Each program module can be operated by installation into an existing application program, or can be operated as an independent program.]